UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/637,431	08/08/2003	Anil Singhal	09851.0006-00000	2626

22852 7590 12/21/2006

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
KIM, JUNG W	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/21/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/637,431	SINGHAL ET AL.	
	Examiner	Art Unit	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-43 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-43 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 4/04.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-43 are pending.

Information Disclosure Statement

2. The IDS submitted on 4/14/04 has been considered.

Specification

3. The disclosure is objected to because of the following informalities: in the Abstract, the second sentence is not grammatical.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 10 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 10 recites the limitation "the third network." There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 40-43 are rejected under 35 U.S.C. 101 because Claims 40-43 are not limited to tangible embodiments. In view of applicant's disclosure, specification page 15, paragraph 50, the medium is not limited to tangible embodiments, instead being defined as including both tangible embodiments (e.g., computer magnetic disk) and intangible embodiments (e.g., carrier wave). As such, the claim is not limited to statutory subject matter and is therefor non-statutory.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vairavan US Patent Application Publication No. 20020083344 (hereinafter Vairavan) in view of Day USPN 7,017,186 (hereinafter Day).

10. As per claims 1-3, Vairavan discloses a method of intrusion detection, comprising:

a. receiving at a probe data packets communicating over a first network link; converting the received data packets into a format suitable for a second network

link; wherein the first network link is a WAN link and the second network link is a LAN and data packets are communicated over a third network link; (paragraph 0047: network device has an access interface that couples one or more WANs and one or more LANs)

b. and monitoring, by the probe, the received packets to evaluate network performance. (paragraph 0090)

11. Vairavan does not disclose transmitting, by the probe, over a second network link, the packets to an intrusion detection system in communication with the second network link. Day discloses an intrusion detection system whereby a probe transmits data packets over a second network link to an intrusion detection system in communication with the second network link. Col. 7:31-40. This setup has the advantage of maintaining a central intrusion detection system for a plurality of network links. Day, col. 7:45-58. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the method of Vairavan to transmit, by the probe over a second network link, the packets to an intrusion detection system in communication with the second network link. One would be motivated to do so to accrue the benefits of a centralized intrusion detection system as taught by Day. The aforementioned cover the limitations of claims 1-3.

12. As per claim 4, the rejections of claims 1-3 as being unpatentable over Vairavan in view of Day are incorporated herein. In addition, Vairavan further discloses the step

of aggregating the data packets received over the first network and the data packets received over the third network. (fig. 1, ports 115(a-g) and interface 120, 125 and 130)

13. As per claims 5-7, the rejections of claims 1-3 as being unpatentable over Vairavan in view of Day are incorporated herein. In addition, Vairavan further discloses the first network link operates using at least one of HSSI protocol, T1 protocol, E1 protocol, ATM protocol, Packet-Over Sonet/SDH protocol, Frame-DS3 protocol, 1G Ethernet protocol, and 10G Ethernet protocol; wherein the first network link comprises a protocol that encapsulates data traffic; wherein the protocol comprises at least one of MPLS protocol, GMPLS protocol, VLAN (802.1q) protocol, HSSI protocol, T1 protocol, E1 protocol, ATM protocol, Packet-Over Sonet/SDH protocol, Frame-DS3 protocol, 1G Ethernet protocol, and 10G Ethernet protocol. (paragraph 0047)

14. As per claims 8-10, the rejections of claims 1-3 as being unpatentable over Vairavan in view of Day are incorporated herein. In addition, Day further discloses the step of maintaining, by the probe, an audit trail buffer for forensic analysis; wherein the audit trail buffer comprises a memory for recording monitored packets; wherein the memory records packets from at least one of the first network link and the third network link. (col. 7:36-40)

15. As per claim 11, the rejections of claims 8-10 as being unpatentable over Vairavan in view of Day are incorporated herein. In addition, Day further discloses the

step of receiving, by the probe, an event notification, communicating, by the probe, the current contents of the audit trail buffer. (col. 7:55-65)

16. As per claims 12 and 13, the rejections of claims 8-10 as being unpatentable over Vairavan in view of Day are incorporated herein. In addition, Vairavan further discloses the converting step comprises: storing received packets in a collection buffer; stripping header information associated with a protocol of the first network link; and adding header information associated with a protocol of the second network link; wherein the step of storing comprises storing packets received from at least one of the first network and the third network link. (Fig. 1: inherent in a protocol conversion from WAN to LAN)

17. As per claim 14, the rejections of claims 12 and 13 as being unpatentable over Vairavan in view of Day are incorporated herein. In addition, the stripping step further comprising stripping header and checksum information associated with a protocol of the first network link and the adding step further comprising adding header and checksum information associated with a protocol of the second network link; wherein the step of storing comprises storing packets received from at least one of the first network link and a third network link are obvious enhancements because different communication protocols utilized different checksum values.

18. As per claim 15, the rejections of claims 12 and 13 as being unpatentable over Vairavan in view of Day are incorporated herein. In addition, the step of stripping comprising stripping at least one of a Layer 2 MAC header, an Ethernet source address, and an Ethernet destination address is an obvious enhancement because Ethernet is conventionally utilized in LAN technology.

19. As per claim 16, the rejections of claims 1-3 as being unpatentable over Vairavan in view of Day are incorporated herein. In addition, Vairavan discloses the method comprises, prior to transmitting over the second network link, filtering a subset of the received packets. (fig. 6A, reference nos. 630-645)

20. As per claims 17 and 18, the rejection of claim 16 as being unpatentable over Vairavan in view of Day is incorporated herein. In addition, it would be obvious for the first network link to comprise an ATM protocol because ATM switching technology is conventionally implemented in WAN networks. Moreover, Day discloses extracting exclusively or inclusively according to pre-configured filter rules and filtering network packets into their constituent components. Col. 8:10:12 and lines 26-38. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the filtering step to comprising filtering packets comprising at least one of management control data such as F4 OAM, F5 OAM, Flow Control, a UNI 3.x frame, a UNI 4.0 frame, a PNNI v1.x frames, and an encapsulation-specific control frame. One would be motivated to do so to selectively deconstruct the network packets for efficient

storage and retrieval means to detect anomalous network behavior. Day, ibid. The aforementioned cover the limitations of claims 17 and 18.

21. As per claim 19, the rejection of claim 16 as being unpatentable over Vairavan in view of Day is incorporated herein. In addition, it would be obvious for the filtering to comprising filtering voice-over IP because Day disclose extracting exclusively or inclusively according to pre-configured filter rules and filtering network packets into their constituent components. Col. 8:10-12 and lines 26-38.

22. As per claim 20, the rejections of claims 16 as being unpatentable over Vairavan in view of Day are incorporated herein. In addition, Vairavan discloses the filtering further comprises filtering based on predetermined criteria and user-defined criteria. (fig. 6A, reference nos. 630-645)

23. As per claims 21-39, the rejections of claims 1-19 as being unpatentable over Vairavan in view of Day are incorporated herein. In addition, Vairavan and Day discloses the first network link comprises a protocol that encapsulates data traffic (WAN link); wherein at least one of the monitored data packets and the converted packets are directed to permanent storage media for 24x7 Network Surveillance and correlation purposes (Day, fig. 1, reference no. 100); wherein at least one of the directed monitored data packets and the directed converted packets are read by a software application.

(Day, fig. 1, reference no. 200). The aforementioned cover the limitations of claims 21-39.

24. As per claims 40-43, they are claims corresponding to claims 1-39, and they do not teach or define above the information claimed in claims 1-39. Therefore, claims 40-43 are rejected as being unpatentable over Vairavan in view of Day for the same reasons set forth in the rejections of claims 1-39.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jk
October 20, 2006

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100